Comments of Thomas D. Sydnor II,
Director of the Center for the Study of Digital Property and Senior Fellow at
The Progress & Freedom Foundation
Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Preserving the Open Internet	)	GN Docket No. 09-191
	)	
Broadband Industry Practices	)	WC Docket No. 07-52

COMMENTS of THOMAS D. SYDNOR II, SENIOR FELLOW AND DIRECTOR OF THE CENTER FOR THE STUDY OF DIGITAL PROPERTY AT THE PROGRESS & FREEDOM FOUNDATION

Thomas D. Sydnor II,
The Progress & Freedom Foundation
1444 Eye Street, NW, Suite 500
Washington, D.C. 20005
January 14, 2010

I. STATEMENT OF INTEREST.

These comments are filed on behalf of Thomas D. Sydnor II, Director of the Center for the Study of Digital Property and Senior Fellow at the Progress & Freedom Foundation, a § 501(c)(3) foundation dedicated to studying the digital revolution in communications technologies and its larger effects upon society. These comments are filed in my personal capacity, so they may not represent the views of the Progress & Freedom Foundation or any of its other Fellows, Board Members, or employees.

I am filing these comments because I have written and published extensively about the sort of file-sharing programs that have been at the center of many recent disputes about the alleged need for so-called "network neutrality" laws or regulations. When I worked for the United States Patent & Trademark Office, I published and testified to Congress about the risks created by "lawful" file-sharing programs and services that are used almost exclusively to download and "share" infringing copies of popular music, movies, books, and software. At PFF, I have continued to identify, publish and testify before multiple Committees of Congress about the risks created by such file-sharing programs and services.

Moreover, my familiarity with administrative law should help me show the Commission why such empirical research implicates the legal duties imposed upon the Commission, or any other federal agency engaged in notice-and-comment rulemaking. Before I entered governmental or public service, I spent 12 years as a litigation attorney in private practice at the D.C. offices of major, national law firms. During that time, I specialized on intellectual-property and administrative-law cases. As a result, in my free time, I am revising and editing a 150+-page legal analysis of how courts determine whether to vacate, remand, or sustain agency action subject to judicial review under Section 706(2) of the Administrative Procedure Act ("APA"), or statutes imposing analogous standards of review. Depending upon the final length of this paper, I plan to publish it as either a series of law-review articles or a short book.

To be clear, I conclude that, as a matter of law, the Commission now lacks any delegated authority to impose binding "network neutrality" rules upon providers of broadband Internet-access services ("ISPs"), particularly at the behest of providers of TCP/IP-based applications, services, or devices ("online service providers, or "OSPs") whom the Commission cannot regulate. Consequently, I join in the Comments on the Commission's lack of jurisdiction filed in this rulemaking by my colleague, Barbara Espin, Senior Fellow and Director of the Center for Communications and Competition Policy at the Progress & Freedom Foundation.

Nevertheless, the rest of my comments will presume, *arguendo*, that the Commission either does have, (or could acquire before this rulemaking concludes), jurisdiction to impose either the Proposed Rules in its NPRM or other rules that could be the "logical outgrowth" of those Proposed Rules. I will adopt this presumption because even if Ms. Espin's jurisdictional analysis is ultimately held to be entirely correct,

any "neutrality" rules that the Commission does promulgate in this rulemaking will, potentially for years, bind broadband ISPs and thus affect not only the development of the Internet, but also the interests of persons, like me, who subscribe to broadband Internet-access services.

Consequently, as a practical matter, even if I conclude that the Commission lacks jurisdiction to promulgate its Proposed Rules, I still have direct professional and personal interests in ensuring that any rules that the Commission does promulgate do as little harm as possible. Any such rules will inevitably affect me not only in my professional capacity, but also in my personal capacity as a father who subscribes to broadband Internet-access services.

For example, in both my personal and professional capacities, I have been encouraging and will keep encouraging providers of broadband Internet-access services—including my current provider—to adopt Terms of Service that would, by default, potentially reduce the costs of broadband Internet-access services for law-abiding families like mine while protecting my family finances, my job, and my children from the profound, (and potentially fatal), risks associated with scores of "lawful" file-sharing programs and services that are only rarely used for any of the "lawful" purposes for which they are so ill-suited. Worse yet, many of these programs are deliberately designed to thwart control at the "end" or the "edge" of the Internet: OSPs deliberately made it needlessly difficult and expensive for either ordinary families like mine or small businesses to prevent their applications and services from being used on our computers or networks.

Moreover, many of these programs not only pose an array of documented risks to the families that subscribe to broadband Internet-access services, they also impose significant burdens upon ISPs themselves. Today, a given ISP's network can become easily congested by unlawful file-sharing traffic that ISPs cannot easily "manage" *because* almost all of that traffic is unlawful. At present, the costs and delays caused by such almost-entirely-unlawful traffic are distributed inequitably among *all* of an given ISP's subscribers—*even though most of those subscribers never use (nor intend to use) any of these problematic file-sharing programs.*

Fortunately, at least before the release of the NPRM, there seemed to be a simple win-win-win solution that could remediate most of these interrelated threats to the wallets of most broadband subscribers, and the personal safety of millions of families and children, the business interests of broadband ISPs, and the federal civil rights of copyright owners: Broadband ISPs could grant a small discount to families that agreed to default Terms of Service that would let their ISP block the use of popular file-sharing programs and services used mostly, (or even almost exclusively), for unlawful purposes. Those few subscribers who wanted to use such programs or services would remain free to use them by acknowledging their risks, forfeiting the default discount, (or paying a cost-related fee), and notifying their ISP to stop blocking them.

Such default Terms of Service would inarguably better serve the legitimate, lawful interests of most families, most ISPs, and most copyright owners—not to mention the interests of both the federal government and the other governmental or private employers that employ diligent or family-focused people who may perform work-related tasks on their home computer. But this almost-everyone-wins

scenario can only occur if broadband ISPs can reasonably conclude that they could also reduce their own costs and burdens by adopting such default Terms of Service.

Sadly, that is the conclusion that the Proposed Rules in the Commission's NPRM would foreclose. In effect, those Proposed Rules state that if any ISP "discriminates" by degrading, blocking, or charging fees to *even the very worst OSPs lurking on the Internet*—those who choose to keep on providing applications or services that are used unlawfully 95% of the time—then the Commission will empower each of these lawless OSPs to file an administrative enforcement action against every ISP that dares to "discriminate" against its 5%-"lawful" applications or services—regardless of whether those ISPs were trying to protect their subscribers from lawsuits, the rule of law itself, or even to just reduce the extent to which their own services were used to facilitate the illegal file-sharing that systematically compromises not only the federal civil rights of job-creating American copyright owners, but also the future of the law-abiding, job-creating American OSPs that are building safe, legal and innovative Internet content-distribution systems like Hulu, iTunes, MySpace, and the current iteration of YouTube.

As a result, even assuming, *arguendo*, that the Commission had jurisdiction to enact the NPRM's Proposed Rules, I conclude that these Rules are arbitrary and capricious because they fail to reflect reasoned decisionmaking. Indeed, these Proposed Rules are both substantively and procedurally defective. Below, I will explain why the Proposed Rules are procedurally defective: they are "mush" that cannot provide reasonable notice of what the Commission proposes to do or how it proposes to do the whatever-it-is that it proposes to do.

I will then explain why I the Commission's Proposed Rules are substantively defective. In short, these Rules repeatedly and egregiously fail to reflect the sort of "reasoned decisionmaking" required whenever an administrative agency uses notice-and-comment rulemaking to impose binding legal obligations.

I will then explain how the Commission could productively and narrow the scope of its Proposed Rules. Doing so would make them less arbitrary and less unreasoned. It would also make them less manifestly destructive not only to the vitality of personal, corporate, national, and military security, but also to vitality of the federal civil rights of U.S. and foreign citizens, including the copyrights that have helped to make U.S. creators and U.S. creative industries, world-leading producers of a vast array of expressive works including news reports, books, music, movies, and application and entertainment software.

II. DISCUSSION.

Providers of Internet applications, services, and devices routinely earn rave reviews from both consumers and experts *because* they engage in the types of "discrimination" that the Commission would denounce if perpetrated by broadband ISPs. These indisputable facts

A. The Proposed Rules are procedurally and substantively defective because they are too vague either to provide the "notice" required for notice-and-comment rulemaking or to reflect reasoned decisionmaking.

The Proposed Rules set forth in the NPRM are stunningly vague. It seems unlikely that an agency can provide the "notice" required to initiate notice-and-comment rulemaking by notifying the public that it intends to require some persons, in some way, to behave reasonably, sometimes. But that is about all that the Proposed Rules propose. Indeed, it thus appears that all of the NPRM's six substantive Proposed Rules could be consolidated into a clearer one-sentence Final Rule:

> **§ 8.5 Reasonableness.**
>
> At least some providers of non-specialized broadband Internet access services may not behave in a way that the Commission will, somehow, later adjudicate to be unreasonable as to any network user, application provider, service provider, device provider, content provider, law-enforcement authority, homeland-security authority, or any public-safety-related obligation.

That sentence captures every nuance and detail provided by the substantive Proposed Rules in the Commission's NPRM. But even it can be further shortened without any real loss of meaning:

> **§ 8.5 Reasonableness.**
>
> At least some providers of non-specialized broadband Internet access services must act reasonably as to others who do or might benefit from its services.

In short, the NPRM has no clothes. The Commission has proposed to codify six "Principles" that would regulate broadband Internet-access providers. Each proposed Principle seems to impose an absolute duty or prohibition that broadband Internet-access providers must *always* observe. But each "Principle" is then "subject to reasonable network management," which the NPRM, (*e.g.*, ¶ 136), effectively defines to include any of the many real-world facts or circumstances that would make it reasonable for broadband Internet-access providers to do what the six Principles seem to say that they cannot do. Moreover, the Commission also acknowledges that its Principles probably must be wholly inapplicable to a completely undefined set of "managed or specialized services."

When combined, these sweeping prohibitions and their ill-defined-but-sweeping exceptions thus create a one-way or one-sided regulatory analog of Immanuel Kant's Categorical Imperative or the Golden Rule: "Providers of some broadband Internet access services must act reasonably as to others who benefit from their services."

Worse yet, the Commission's Proposed Rules are even more vague than a true regulatory Golden Rule. Some of them may not apply, at all, to some broadband ISPs, particularly those providing mobile broadband-access services. Moreover, none may be applicable to a completely undefined set of "managed or specialized services." And even when the duties of reasonableness imposed by the Proposed Rules apply, critical aspects of their content and enforcement.

For example, assume *arguendo*, that under some circumstances, administrative law might allow an agency to impose a one-sided regulatory Golden Rule even though the duties of reasonableness thus imposed would remain wholly inchoate until defined by subsequent enforcement actions.

The problem with a regulatory Golden Rule is that it is extremely vague. Nevertheless, while it is difficult to dispute that reasonable people should behave reasonably, it certainly is possible to enforce or impose a duty of reasonableness through procedures that would be *unreasonable.* In other words, if the Commission could impose a one-sided regulatory Golden Rule whose content would be determined during subsequent adjudications, it is difficult to see how it could do so if the adjudicatory process to be used was wholly undefined, as is the case here.

For example, the odd structure of the Proposed Rules heightens the importance of a question that the NPRM neither acknowledges nor answers: In an action to enforce the Proposed Rules, who would bear the burden of proving that a covered ISP's conduct was or was not reasonable?

Indeed, not only does the NPRM fail to acknowledge the significance of this question and answer it openly, it becomes wholly incoherent just when it might have been addressed. This happens in NPRM ¶¶ 109-110, in which the Commission openly contradicts itself.

In these Paragraphs, the Commission struggles with the serious question raised by the odd structure of its Proposed Rules. The Commission admits that the Proposed Rules prohibit *unreasonable* episodes of types of ISP conduct that often could, in practice, be reasonable or unreasonable. But if so, then why does it make any sense to produce such a result through the potentially misleading and needlessly convoluted process of enacting rules that, in one part, impose (as the NPRM puts it) "unqualified" prohibitions against particular types of ISP conduct—both reasonable and unreasonable—and then, in another part, quietly mutter that, well, those prohibitions will be inapplicable whenever enforcing them would be unreasonable?

In Paragraphs 109 and 110, the Commission tries to rationalize this regulatory Rube-Goldberg machine. The NPRM explains that, yes, it realizes that throughout legal history, reasonable law-makers seeking to produce the results that the Commission does seek to produce here have long chosen to produce such results by enacting laws that proscribe only "unjust" or "unreasonable" conduct. The NPRM then tries, (¶ 110), to explain why this familiar, say-what-you mean approach to drafting legal duties was rejected here: "We believe that a bright-line rule against discrimination, subject to reasonable network management and enumerated exceptions, may better fit the unique characteristics of the Internet, which differs from other communications networks in that it was not initially designed to support just one application (like telephone and cable television networks), but rather to allow users at the edge of the network to decide which lawful uses to direct the network."

That explanation explains nothing because it makes no sense at all. It is wholly nonresponsive: the now-mostly irrelevant intentions of long-dead engineers cannot explain the regulatory circumlocutions of living lawyers. It also contradicts virtually everything said about the effects of the Proposed Rules in the NPRM: Were the use of "bright-line rules" really demanded in this context, then the NPRM is self-immolating. Its central argument also confounds common sense: it argues that even though "bright line" rules were always found inappropriate even back in the simpler days when communications networks were designed for narrow, specialized, predictable purposes, bright-line rules are now

appropriate *because* the purposes for which communications networks like the Internet will be used are general, unpredictable, and constantly changing.

As a result of such facially unreasoned and unreasonable illogic, commenters can only guess why the Proposed Rules were structured in a way that made them potentially misleading and unnecessarily convoluted. Indeed, increased vagueness seems to be only potential advantage to such circumlocution: While rules imposing familiar prohibitions against unreasonable behavior would clearly not impose the burden of proving reasonableness upon the challenged ISP, the structure of the Proposed Rules makes it essentially impossible to guess which party would bear the burden of proof on the critical issue of reasonableness.

Similar problems of vagueness recur throughout the NPRM. For example, Proposed Rule 8.13 states, "Subject to reasonable network management, a provider of broadband Internet access services must treat lawful content, applications, or services in a nondiscriminatory manner." In U.S. law, undefined terms in laws are strongly presumed to have their ordinary meaning. If "nondiscriminatory manner" had its ordinary meaning, then it would appear to prohibit an ISP from (1) by default, blocking all of its subscribers from accessing or using a lawful application or service; or (2) blocking all subscribers from accessing or using a lawful application or service unless they paid an extra fee.

But this term may not have its ordinary meaning, at least for now. The NPRM explains that the Commissioners proposing this Proposed Rule "understand" the phrase "nondiscriminatory manner" to mean something far narrower than what the phrase would ordinary mean:

> We understand the term "nondiscriminatory" to mean that a broadband Internet access service provider may not charge a content, application, or service provider for enhanced or prioritized access to the subscribers of the broadband Internet access provider…. We propose that this rule would not prevent a broadband Internet access service provider from charging subscribers different prices for different services.[1]

But only promulgated rules—not statements in an NPRM—actually state laws that bind the Commission until changed. Consequently, only a *codified* specialized definition of "nondiscriminatory manner" would obligate the Commission to apply this specialized definition of "nondiscriminatory manner"—unless or until it conducted further rulemaking.

In conclusion, the Proposed Rules not only propose to impose a one-sided regulatory Golden Rule, the propose to do so in ways that repeatedly make the scope and the enforcement of it even more needlessly vague than it would inevitably be. Particularly in light of the non-explanation of the basic structure of the Proposed Rules, serious procedural questions thus arise. As the D.C. Circuit once noted: "To allow an agency to play hunt the peanut with technical information, hiding or disguising the

[1] NPRM, ¶106.

information that it employs, is to condone a practice in which the agency treats what should be a genuine interchange as mere bureaucratic sport."[2]

The notice-and-comment obligations imposed by the Administrative Procedure Act ("APA") require the Commission to fulfill three basic obligations before it can lawfully regulate Internet-access providers. First, the Commission must give meaningful notice of what legal duties it proposes to impose. Second, the Commission must provide a meaningful opportunity for the potentially afflicted to comment upon its proposals. Third, the Commission must engage in reasoned decisionmaking when confronting the resulting record and crafting any final rules.

D.C. Circuit precedent strongly suggests that the Commission violated all three of these obligations when it proposed to impose a particularly and needlessly extra-vague one-sided regulatory Golden Rule upon providers of broadband Internet-access services:

> A substantive regulation must have sufficient content and definitiveness as to be a meaningful exercise in agency lawmaking. It is certainly not open to an agency to promulgate mush and then give it concrete form only through subsequent less formal "interpretations…." That technique would circumvent section 553, the notice and comment procedures of the APA.[3]

That is, however, is just what the NPRM proposes to do.

B. The Commission Should Not "Commoditize" Internet-Access Services by Imposing Precautionary "Neutrality" Regulations at the Behest of Producers of Complementary Goods.

In addition to procedural and substantive vagueness issues, the NPRM also seems to overlook or ignore potentially critical aspects of the very complex and critical disputes that it tries to mediate.

1. The NPRM does not acknowledge that calls for one-way "Net Neutrality" laws could be anticompetitive attempts to commoditize producers of a complementary good or service.

There are disturbing contradictions inherent in claims that we need laws that require ISPs to behave fairly towards OSPs because ISPs, unlike OSPs, could well cause the "open Internet" to degenerate into something as sterile, oppressive, and non-transparent as Google's search engine, Amazon.com's store,

---

[2] Gerber v. Norton, 294 F.3d 173, 181 (D.C. Cir. 2002) (quoting Connecticutt Light & Power Co. v. NRC, 673 F.2d 525, 530 (D.C. Cir. 1982)).

[3] Paralyzed Veterans of Am. v. D.C. Arena L.P., 117 F.3d 579, 584 (D.C. Cir. 1997); see also Checkosky v. SEC, 139 F.3d 221, 224 (D.C. Cir. 1998) ("Elementary administrative norms of fair notice and reasoned decisionmaking demand that the Commission define [the circumstances in which negligent accounting may constitute improper professional conduct] with some specificity. It has not done so."); id. at 226 ("When an agency utterly fails to provide a standard for its decision, it runs afoul of more than one provision of the [APA]."); ACLU v. FCC, 823 F.2d 1554, 1573 n. 38 (D.C. Cir. 1987) ("waiver provisions cannot do service for reasoned decisionmaking").

or Apple's iPhone, (all "closed" platforms, services, or devices). Such contradictions suggest the need to consider whether the teachings of the *Noerr-Pennington* doctrine may be relevant to this proceeding. This doctrine teaches that—antitrust laws notwithstanding—there is a perfectly legal way for entities with market power to conspire as a cartel in order to impose unreasonable restraints of trade upon competitors or producers of complementary goods: They need only convince a governmental to impose the unreasonable restraint.

For example, railroads displacing stage coaches as a more efficient technology for transporting large volumes of freight over long distances provide a classic example of "Schumpeterian" completion-by-innovation. But the relentless cascade of *productive* innovation that Schumpeterian competition inspires among *law-abiding* businesses soon created a technology and a business model that could often out-compete railroads—long-haul trucking companies. As a result, owners of railroads did what entrenched, law-abiding incumbents should do when facing competition from a newer and often-more-efficient technology: They conspired to convince governments to regulate the life out of long-haul trucking companies.

In *Eastern Railroad Presidents Conference v. Noerr Motor Freight, Inc.,* the Supreme Court dismissed the long-haul trucking companies' antitrust lawsuit against the railroads and held—correctly—that not even antitrust laws trump the First Amendment right to petition the government for the redress of grievances—even those against competitors who could compete just a bit too effectively unless hamstrung by punitive laws.[4] *Noerr* and similar cases thus contain a powerful warning to all government employees and officials: It is perfectly legal for entire industries to conspire together in cartel-like style *for the purpose of imposing unreasonable restraints of trade upon others*—provided that they can get *you* to enact the unreasonable restraints as laws.

Unfortunately, while *Noerr* is a paradigm case, it is also an easy case. If industries A and B directly compete in the same market using different technologies, then almost all honest legislators, administrators, or judges would probably become quite skeptical were industry A to argue that "the public interest" requires the government to impose crippling regulations upon the technology used by Industry B.

Nevertheless, common sense and basic economics dictate that fundamentally similar—but far more subtle—*Noerr*-like efforts to convince government to impose unreasonable restraints on technologies used by other producers should and do occur among producers of *complementary* goods.[5] ISPs and OSPs are good examples of such "complementary" producers: the value that users derive from the Internet is inarguably derived partly from the productive activities of ISPs and partly from the productive activities of OSPs.

Producers of complementary goods are neither precisely alike, nor entirely different from, direct competitors. They are like direct competitors because they do compete against each other to capture the largest possible share of the revenue potentially generated by their mutual efforts. At least in the

[4] 365 U.S. 127 (1961).

[5] Dictionary of Economics 66 (4th ed., Bloomberg Press, Graham Bannock, et al., eds., 2003).

short run, this competition is a traditional, zero-sum, win-lose game: if two entities produce complementary goods or services, revenue captured by one will almost inevitably reduce the revenues that *could* be captured by the other.

But producers of complementary goods differ from direct competitors because their conflicts and machinations are more subtle. For example, long-haul trucking companies were direct competitors to railroads. Consequently, the Eastern Railroads Presidents' Association would have happily sought laws so punitive that they would have utterly *destroyed* the viability of business models based upon long-haul trucking technologies.

By contrast, producers of complementary goods, (even though they do compete against each other in some ways), still need each other. If Industry A and Industry B produce complementary goods, neither should want the government to enact laws that would *destroy* the other. Nevertheless, either industry might well want the government to enact laws that would tend to *commoditize* the good or service produced by the other. After all, such laws would tend to drive profits in the other industry towards marginal costs, and that would increase the amount of revenues that could be potentially captured by producers of a complement.

The NPRM notes that OSPs argue that the design of the Internet embodies a quasi-mystical "end-to-end" principle that dictates that the broadband ISPs who provide services complementary to those of OSPs must be legally obligated to act similarly and in a non-discriminatory manner towards essentially all OSPs. Such ISP-only "neutrality" regulations might not *destroy* the providers of broadband Internet-access services. But they would predictably tend to *commoditize* providers of broadband Internet-access services: they would favor innovation at the "edge," rather than in the network, and this should tend to drive ISPs to compete against each other mostly to see who could become the biggest dumb fungible bit-pipe among those providing big, dumb fungible bit-pipes.

In short, "neutrality" rule that would tend to commoditize ISPs while imposing no duties upon OSPs do seem to look like the sorts of laws that providers of complementary goods might be too eager to have imposed upon others who provide goods or services complementary to their own.

Nevertheless, the problem here is not that OSPs supporting ISP-only "neutrality" regulations are necessarily acting in bad faith. Nor is it that the Commission has necessarily been duped into proposing an unreasonable restraint of trade. Rather, the problem is that the NPRM and Proposed Rules do not seem to acknowledge this disturbing aspect of the very important, complex, high-stakes problem that they purport to mediate.

2. One-Sided Regulation of a Two-Sided Market Is Inherently Impractical.

In its NPRM, the Commission admits that "the Internet is an example of a 'two-sided market,' in that broadband Internet access service providers offer service to both end-user customers and to content,

application, and service providers simultaneously."[6] The NPRM then discusses in great detail mostly hypothetical examples of how ISPs could behave unreasonably when they "offer service to" OSPs.

Nevertheless, the Proposed Rules' exemptions for "reasonable network management" at least implicitly recognize the converse proposition: Just as ISPs could behave, (and in rare cases, may have behaved) unreasonably towards OSPs or the ISP's own subscribers, so too could OSPs behave unreasonably toward ISPs or ISP subscribers. Indeed, far too many OSPs have actually done so—and often through means so malign that they achieved the once-inconceivable result of converting the piracy of popular music and movies into a severe, pervasive and documented threat not only to personal, corporate, military, and national security generally, but also into specific, documented threats to the safety of the daughters of every U.S. President sworn into office during this millennium.[7]

This regulatory asymmetry reveals another fundamental defect in the Proposed Rules that will tend to require them to be and to remain extremely vague and case-specific. The Proposed Rules would impose one-sided regulations upon a two-sided market. In effect, they would require ISPs to behave reasonably toward OSPs who would have no corresponding legal duty to behave reasonably towards ISPs or ISP subscribers.

Unfortunately, the NPRM neither acknowledged to distinguished the potential for debacle inherent in one-sided regulation of a two-sided market. For example, imagine that the NCAA were to change the rules of college football in two narrow respects: (1) the rules of college football would be enforced only against the home team, and (2) if the visiting team or the officials identified a rules violation by the home team, then the home team could avoid any penalty by convincing officials—not that it had obeyed the rules of college football—but that it violated them because the visiting team had behaved in a way that made doing so reasonable.

Naturally, the NCAA would never make such changes. Enforcing rules of "fair play" against only one of two parties who could potentially treat the other unfairly is absurd. Moreover, making the applicability of rules of "fair play" depend upon the behavior of an entity not bound to obey them merely suggests that those rules were neither "fair" nor necessary.

Nevertheless, the Proposed Rules would do something similar as between ISPs and OSPs. And while the Commission does seem to realize that it would impose upon ISPs duties of reasonableness towards OSPs who would remain free to act unreasonably towards ISPs, their subscribers or both, the NPRM never acknowledged the obvious question thus raised: Why, in this particular context, should the inherently risky course of imposing one-sided regulations upon a two-sided market be expected to produce socially beneficial results? Failing to acknowledge or address obvious aspects of a problem is the essence of unreasoned decisionmaking.

Moreover, it should be particularly difficult to conclude that such one-sided regulations would make sense *unless* the one-sidedly regulated were, in fact, the only participants in this two-sided market who

[6] NPRM at ¶ 66 & n. 155.
[7] See infra, [CROSS-REF].

were likely to behave unreasonably. The NPRM fails to show that the potential for OSP, (as well as ISP), misconduct was assessed. Worse yet, such an assessment could easily illustrate the risks of imposing one-sided regulations upon some ISPs in order to protect a class of OSPs that would include many whose own conduct has been as ruthlessly malign as it has been practically harmful.

In conclusion, the structure of the Proposed Rules strongly suggests the possibility that they will force ISPs to become *unreasonably* indulgent of OSPs. The NPRM recognizes that some forms of ISP "discrimination" are entirely reasonable—without *prescribing* any examples of what those might be. Nevertheless, whenever any ISP arguably "discriminates" against any OSP, the Commission, the OSP, any user, or any public-interest group may or may not be able to bring an enforcement action charging that such acts establish a *prima facie* case of unlawful wrongdoing. If the charging party prevails, then the ISP in question will be held by its regulatory agency to have Broken Federal Law by Discriminating Unreasonably Against an OSP, and will face whatever penalties the Commission, and other applicable laws, impose.

By contrast, if the ISP wins, then the adjudicator will find that the ISP's acts were not as unreasonable as they seemed, and dismiss the case. Should that happen, the OSP in question could, of course, quickly re-jigger its application to design around the dismissal's rationale and then file another enforcement action against the same, or a different, ISP. As a result, any OSP filing a "neutrality-enforcement action" against an ISP could fairly describe the possible range of outcomes as follows:

"Heads, I win. Tails, you don't. And I can just sue you again. Shall we continue?"

This sort of inherently biased, one-sided regulatory process should inevitably deter ISPs from engaging in reasonable, socially beneficial forms of "discrimination" against malfeasant OSPs.

C. Reasonable Neutrality Rules Should Protect *Only* Applications, Services or Devices Shown To Be Used *Predominantly* for Lawful Purposes.

While debates about the need for network neutrality laws or rules have tended to be impassioned, I hope that even the most committed proponents and opponents can applaud the aspirations for the Internet that the Commission has expressed. In the NPRM, (¶ 139), the Commission recognizes that an open *and law-abiding* Internet will best promote the growth of our economy and overall broadband ecosystem.

But to hasten the start of the economic growth that a law-abiding Internet would deliver, the Commission should narrow the scope of the Proposed Rules. Reasonable "neutrality" rules need not—indeed, cannot—protect even those OSPs and network "users" who provide or use applications or services that are "lawful"—but are also used *unlawfully* over 90% of the time. Indeed, nothing in the NPRM even suggests why the Commission cannot determine now, without resort to adjudication, that it would do more good than harm by precluding or discouraging ISPs from "discriminating" against applications or services used for unlawful purpose over 90% of the time. The math simply does not add up.

Considing this, or other, viable and narrower alternatives to potentially overbroad solutions is an indispensible element of reasoned decisionmaking. For example, in *Motor Vehicle Manf's Ass'n of the U.S., Inc. v. State Farm Mut. Automobile Ins. Co.,* the Supreme Court unanimously vacated agency rules because an agency had failed to consider obvious, intermediate alternatives to its action.[8] Similarly, in *City of Brookings Mun. Tel. Co. v. FCC,* the D.C. Circuit reminded the Commission that whenever it has failed to acknowledge and discuss obvious alternatives to its actions, such unreasoned decisionmaking "has led uniformly to reversal."[9]

These bedrock principles of administrative law make it essential to consider narrower, and potentially more effective, alternatives to the NPRM's Proposed Rules. The Proposed Rules are about as broad as they could be: in effect, they propose that broadband ISPs should be legally obligated to behave "reasonably" toward *all* "users" of their services and toward *all* OSPs whose applications, services, and devices are "lawful"—even though the NPRM cites no evidence suggesting that the set of OSPs that provide "lawful" TCP/IP-based applications, services and devices differs materially from the set of *all* OSPs that provide TCP/IP-based applications, services and devices. .

The Proposed Rules already recognize that ISPs should be allowed to discriminate against OSPs or "users" whenever such discrimination would be reasonable. But if an application, service or device is used *predominately* for unlawful purposes, then any ISP that blocks or degrades, or otherwise creates any disincentive to provide or use that application, service, or device will almost *necessarily* do more social good than social harm. Acts that do more good than harm are reasonable even under the Golden Rule or the Categorical Imperative.

For example, suppose that an ISP blocks or degrades the use of an application or service used *predominately* for illegal purposes. This ISP would, by definition, be doing more good than harm: more often than not, the ISP's actions would prevent, hinder, or discourage acts that U.S. law deems socially destructive. Nor would it matter whether this ISP acted as a result of the most selfless respect for the sanctity of law, or as a result of the most selfish desire to minimize its own costs and maximize its own revenues by reducing congestion on its network. In either case, the ISP's blocking or degrading such an application or service would still, on balance, do more social good than social harm.

Nor can the current Proposed Rules be defended by claiming that while they *seem* to provide anti-discrimination protections to OSPs and users against whom it would almost always be reasonable for ISPS to "discriminate," they are still reasoned because they would let the Commission conclude, in a

[8] 463 U.S. 29 (1983) (vacating the decision of an agency that rescinded a passive-restraint standard for new cars because it doubted the efficacy of one of the two technologies that could be used to satisfy the standard—without considering the obvious intermediate alternative of simply requiring the use of the other effective passive-restraint technology).

[9] City of Brookings Mun. Tel. Co. v. FCC, 822 F.2d 1153, 1169 (D.C. Cir. 1987); see also, e.g., Int'l Ladies Garment Workers' Union v. Donovan, 722 F.2d 795, 817 (D.C. Cir. 1983) ("an 'artificial narrowing of options is antithetical to reasoned decisionmaking and cannot be upheld'").

.

later adjudication, that such discrimination would actually constitute "reasonable network management."

That misses the point. As one sitting Supreme-Court Justice noted while serving on the D.C. Circuit, an agency rulemaking cannot reasonably decline to promulgate rules that the record reveals to be reasonably just because their equities could be belatedly acknowledged during subsequent adjudications:

> General rules need not work perfectly in all their applications; or to put it more precisely, overall perfection is not best pursued by requiring the delay and expense of case-by-case determination when generic treatment would almost invariably produce the same result.[10]

Moreover, arguments against extending neutrality protections to all broadband "users" and to all OSPs that provide applications services and devices used predominantly for unlawful purposes need not rely upon the abstract premise that ISPs discriminating against applications or services used for predominantly unlawful purposes will necessarily do more good than harm. Practical experience with real applications and services provided by some of the very OSPs whom the Commission's Proposed Rules would protect has repeatedly proven this thesis to an extent unimaginable just over a decade ago. For example, in 1999, reasonable, informed people should have burst out laughing someone suggested that music piracy could end up endangering the children of the President of the United States.

Today, no one is laughing. Between 2000 and 2010, file-sharing programs used almost exclusively to download infringing copies of popular music, movies, images, and software were used in ways that endangered both the daughters of President George W. Bush and the daughters of President Barack Obama—not to mention the daughters of my own and many other millions of far-more ordinary American families. Moreover, the OSPs that compromised the safety of so many children were providing applications or services functionally indistinguishable from those that the Commission recently condemned Comcast for "degrading."

Consequently, the Proposed Rules cannot reasonably force ISPs to undergo the uncertainties, costs, and risks of litigating many enforcement actions just to prove the obvious: it is entirely reasonable for ISPs that choose to do so to "discriminate" against OSPs that have behaved so badly that they turned piracy of popular music into a documented, widespread threat not only to the safety of children, but also to personal, corporate, national and military security.

The reasoned way forward from this unfortunate situation involves *narrowing the scope* of the Proposed Rules. Reasonable net-neutrality rules need not—and cannot—protect even those OSPs whose applications, devices and services are used mostly for unlawful purposes. "Lawful" music-downloading services like those of Amazon.com and iTunes differ radically from "lawful" applications or services like

[10] Illinois Comm. Comm'n v. ICC, 776 F.2d 355, 359 (D.C. Cir. 1985) (Scalia, J.). In the same case, then-Judge Scalia also noted that if an issue is relevant to the question of what decision an agency should make when promulgating rules, then "to make the decision now and consider the issue later is neither rational nor permissible under the APA." Id. at 363.

LimeWire, Morpheus and Isohunt. And the critical difference is painfully simple: the latter set of "lawful" applications and services are almost never used for lawful purposes. Reasoned neutrality rules *must* account for these vast differences among real-world OSPs. As a result, reasoned rules should not prevent or discourage ISPs from "discriminating" in favor of the most law-abiding OSPs or against those whose applications, services or devices are only rarely used for lawful purposes.

Consequently, the Commission should amend its Proposed Rules so that neutrality regulations would protect only those users and providers of applications, services, or devices who bear the burden of proving that their applications, services, or devices are used predominantly for lawful purposes and do not harm a given ISP's network or interests. By thus narrowing the set of OSPs that the Proposed Rules would protect, the Commission could significantly reduce their current potential to unduly burden affected ISPs. This approach would also offer at least five additional advantages.

First, it would provide a means to remedy concerns about inconsistencies and overbreadth imported into the Proposed Rules from the text of horatory "Principles" that were somewhat loosely drafted because they were never intended to state binding legislative rules.

Second, this approach would acknowledge nearly indisputable realities. Unless an OSP can prove that its application, service or device is used predominantly for lawful purposes, then it should be presumptively reasonable for any ISP to block, degrade, impose fees upon, or otherwise "discriminate" against that OSP's application, service or device. It is eminently reasonable for ISPs to "discriminate" against OSPs that provide dangerous toys to children, and reasonable neutrality rules should not prevent or discourage them from doing so.

Third, this approach would acknowledge that real-world experience proves not only that discriminating against applications, services and devices used predominantly for unlawful purposes is almost inevitably reasonable in theory, but even more so in fact. Far too many OSPs have proven not only that applications and services used predominantly for unlawful purposes will tend to be used almost exclusively for unlawful purposes, but also that these applications and services will tend to impose a wide array of risks and costs upon their users, ISPs and society generally. For example, during the past decade, many OSPs built businesses based predominantly the unlawful commerce called "copyright infringement." Time and again, the real-world results of such efforts proved far more dangerous to a far broader range of social interests than anyone could have imagined.[11] Consequently, reasoned neutrality rules should not prevent or discourage ISPs from blocking or degrading access to applications and services used predominantly for unlawful purposes—particularly if blocking these applications and services by default would prevent the identity theft, potential job loss, and costly lawsuits that can occur

[11] Compare, Grokster, 545 U.S. at [CITE] (Breyer, J., concurring) (opining that Gnutella-based file-sharing programs like Morpheus would soon develop many non-infringing uses), with Brian Krebs, Justice Breyer Is Among Victims in Data Breach Caused by File Sharing, The Washington Post (July 9, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html (discussing how someone using the Gnutella-based file-sharing program LimeWire ended up broadcasting Justice Breyer's private financial data over the Internet).

when parents do not know that their children have installed potentially dangerous file-sharing programs.

Fourth, applications, services and devices used for predominantly unlawful purposes also frequently impose many unjust burdens upon ISPs. These burdens also make it even more reasonable for ISPs to discriminate against OSPs whose applications, services, or device are used mostly for unlawful purposes. For example, the distributors of the LimeWire file-sharing program have submitted sworn testimony to Congress asserting that the only effective way to remediate the mess made by the distributors of file-sharing programs like LimeWire and Shareaza would be for Congress to require copyright owners and ISPs like Comcast, AT&T and Verizon to bear *all of the costs* incurred in cleaning up the mess knowingly made by OSPs that keep on distributing lawful-but-largely-lawless file-sharing programs like LimeWire.

Fifth, and finally, this approach would better effectuate the Commission's commendable intent to avoid enacting net-neutrality rules that could prevent ISPs from deterring the infringement of the copyrights—the federal civil rights—that have helped to create millions of American jobs by enabling America's creators and creative industries to become the world's most successful exporters of a vast array of expressive works that include music, movies, images, books, and entertainment and application software.

1. The Proposed Rules are incoherent and overbroad.

Because the Commission's Proposed Rules merely codify and expand 2005 "Principles" that were never meant to prescribe binding legislative rules, the Proposed Rules are facially incoherent and overbroad. Proposed Rules 8.5, 8.7 and 8.13 provide "neutrality" protections only to "lawful" content, applications, or services. But Proposed Rule 8.9 is much *narrower*: it protects only "lawful" devices "that do not harm the network" and it does not prevent ISPs from discriminating against providers or users of such devices. Yet Proposed Rules 8.11 and 8.15 are far *broader*: they would protect OSPs that provide applications, and services *even if* what they provide is *entirely* unlawful. And while ISPs would ordinarily have legal duties only toward their "subscribers," Proposed Rules 8.5, 8.7, 8.9, and 8.15 would impose upon ISPs duties toward all "users"—regardless of whether those "users" are using applications, services or devices that the ISP's actual subscribers do not want to be used by "users" of the Internet-access services that they have procured from a broadband ISP. As a result, the Proposed Rules are now internally incoherent in part and facially overbroad in part.

First, the Proposed Rules are internally incoherent in their scope. For example, Proposed Rule 8.9 potentially protects devices only if they are both "lawful" and do not "harm the network." But even then, it states only that an ISP must allow "any of its users" to run and use any lawful, non-network-harming device: Rule 8.9 does not require ISPs to behave "in a nondiscriminatory manner" towards device users who choose to do so.

Nevertheless, the same Proposed Rules potentially protect "lawful" applications, and services *even if* they "harm the network," and they require ISPs to treat all such applications and services in a "nondiscriminatory manner" *regardless* of whether such applications or services "harm the [ISP's}

network." Predictably, the NPRM fails to identify any reason why reasonable experts would prevent or deter ISPs from discriminating against "lawful" applications and services that do "harm the [ISP's] network" while leaving those same ISPs free to discriminate against even those "lawful devices" that do not "harm the [ISP's] network." Indeed, no such rationale seems conceivable, especially since most "devices" could be implemented as "applications" or as "services"—or vice versa.

Nor are these the only internal-incoherence problems in the Proposed Rules. For example, the NPRM fails to explain why some of the proposed neutrality rules (but not others) would protect even providers of wholly *unlawful* applications, services, devices, or content. Proposed Rule 8.15 would prevent or discourage ISPs from being insufficiently "transparent" even toward OSPs that provide *wholly unlawful* applications, services, devices, or content. Proposed Rule 8.11 would prevent or discourage ISPs from depriving "any of its users of [their] entitlement to competition" among *all* "network providers, application providers, service providers, and content providers"—regardless of whether those "providers" were entirely law-abiding or wholly unlawful. Consequently, both rules are facially overbroad and unreasoned. Except in special circumstances, (like those relating to persons accused of criminal acts), reasoned laws should not protect the wholly lawless.

Second, the Commission's Proposed Rules are also arbitrarily overbroad: they would impose upon ISPs "neutrality" obligations toward all "users" of their networks. This seems legally suspect, and it could often be affirmatively counterproductive in practice. At most, any neutrality rules imposed upon ISPs should extend only to those who "subscribe" to broadband Internet-access services.

After all, subscribers and the ultimate "users" of the Internet-access services that a subscriber purchases may have very different—indeed, conflicting—ideas about how that access should be used. For example, parents or small businesses that subscribe to broadband Internet-access services may not want "users" like children or employees to run potentially dangerous applications like file-sharing programs. It would be affirmatively destructive to impose upon ISPs duties towards "users" that would require ISPs to assist, or even just discourage them from deterring, the designs of "users" trying to thwart the acceptable-use or security policies of an ISPs' actual "subscribers."

For example, in my personal capacity as a father, husband, and homeowner, I subscribe to broadband Internet-access services. Were my broadband ISP willing to do so, I would happily authorize my ISP to block (or just delay) any network "user's" attempt to use *my* Internet-access account to run potentially dangerous file-sharing programs like LimeWire or Shareaza or to access websites like Isohunt. I would authorize such "discrimination" for the same reason that many colleges and universities do so by default: I know perfectly well that such programs and websites are almost never used *mostly* for lawful purposes.

Nevertheless, were the Commission to promulgate its Proposed Rules, my ISP could violate its one-sided "neutrality" duties were it to do what its subscriber wanted by blocking "users" of its network from using my account, (and my computers), to run dangerous (but "lawful") file-sharing programs or to access dangerous (but "lawful") websites. Indeed, as a result of OSP efforts to thwart the Internet's

alleged "end-to-end" principle, ISPs may often be far better situated than individual persons, families, small-businesses or government agencies to help design and enforce acceptable-use policies.[12]

2. Reasoned net-neutrality rules cannot protect OSPs providing applications, services, or devices used unlawfully most of the time because it is, by definition, almost inevitably reasonable for ISPs to discriminate against them.

The Commission's Proposed Rules recognize that "neutrality" obligations should be inapplicable whenever it would be reasonable for an ISP to discriminate against an OSP. Generally, "reasonable" conduct must do more good than harm. For this reason, laws prohibit only conduct that tends to do more harm than good. Consequently, reasoned net-neutrality rules should neither prevent nor discourage ISPs from discriminating against OSPs that provide applications, services, or devices that are predominantly used for unlawful purposes. Virtually by definition, ISPs discriminating against such OSPs would do more good than harm.

For example, the NPRM states, (¶ 139), "[I]t is important to remember that open Internet principles apply only to lawful transfers of content. They do not, for example apply to activities such as the unlawful distribution of copyrighted works, which has adverse consequences on the economy and overall broadband ecosystem." Consequently, if a "lawful" application or service—like the Gnutella-based file-sharing program Morpheus—is used for the unlawful distribution of copyrighted works 95% of the time, then an ISP would do surely do more good than harm by blocking or degrading it.[13]

As a result, reasoned net-neutrality rules promulgated by a federal law-enforcement agency like the Commission to protect "open Internet principles" should not prevent or discourage ISPs from disadvantaging applications, services, or devices used mostly for the unlawful purposes that actually undermine the very "open internet principles" that these rules supposedly protect.[14]

---

[12] See Overexposed: The Threats to Privacy and Security on Filesharing Networks: Hearing Before the H. Comm. on Government Reform, 108 Cong. 25-38 (2003) (university network managers testify that "P2P software is commonly designed to circumvent network security systems).

[13] To be clear, these comments do not propose that the Commission should require or otherwise legally obligate any ISP to discriminate against, block, degrade, charge or otherwise discriminate against any given OSP. Rather, they propose only that the Proposed Rules should be narrowed to ensure that they do not prevent or discourage ISPs otherwise willing to experiment to devise effective, proportionate means of deterring unlawful uses of applications and services used predominately for unlawful purposes.

[14] This predominant-use approach to narrowing the Proposed Rules derives exclusively from the simple reasoning set forth above. It is neither derived from, nor intended to mirror or endorse, any interpretation of any standard for imposing or withholding legal liability developed within the law of anti-circumvention protections or copyrights, including any related to the latter's still-opaque capacity-for-substantial-noninfringing-use test. See Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 442 (1985); see also MGM Studios, Inc. v. Grokster, 545 U.S. 913, 934-35 (2005) (noting, but not resolving, a circuit-court split over the meaning of the Sony test).

In theory, this abstract balancing should suffice to show why a federal law-enforcement agency like the Commission should not enact rules that could prevent or discourage law-abiding ISPs from "discriminating" against applications, services, or devices used predominantly to violate federal law. But in this case, that conclusion need not rest upon mere theory.

Sadly, the Internet of the moment has provided far too many real-world examples of applications and services that are used for unlawful purposes—not just predominantly, but almost exclusively. In practice, these 95%-unlawful applications and services have proven to be far more malign than any mere "theory" would suggest.

3. In practice, applications and services used mostly for unlawful purposes have often imposed upon children and families risks so severe, diverse and numerous that reasoned laws can never prevent or discourage ISPs from "discriminating" against such applications or services.

To the contrary, both domestically and internationally, ISPs and copyright owners have been experimenting with an array of interesting means they propose only

a) Close cases would rarely arise were neutrality rules to protect only applications, services and devices used predominately for lawful purpose.

Existing evidence proves that if the Commission provided neutrality protections only to OSPs providing applications, services, and devices used predominately for lawful purposes, it would rarely, if ever, have to adjudicate close cases in which it was unclear whether a given OSP was entitled to the Commission's neutrality protections. The needs of lawful and unlawful commerce differ profoundly. Consequently, the Commission should rarely have difficulty discerning whether a given application, service, or device is used for predominately lawful purposes.

This point has been proven repeatedly in cases involving distributors of what could be called "piracy adapted" programs or services. As the term is used here, "piracy-adapted" file-sharing programs, protocols, and websites include those that happen to be—intentionally, knowingly, recklessly or negligently—well-suited to the needs of users who want to use them to infringe copyrights in popular music, movies, software, books and images.

While careful analyses of how applications that could be used mostly for unlawful purposes actually are used in practice have been rare, their results of those that have been done have been quite consistent.

For example, in *A & M Records, Inc. v. Napster, Inc.,* the district court found, and the appellate court affirmed, a statistical analysis that showed that 87% of the files available on the Napster network were copyrighted.[15]

Similarly, in *In re Aimster,* the court found no evidence of non-infringing use of the defendant's file-sharing application.[16]

[15] See, e.g., A&M Records, Inc. v. Napster, Inc., F.3d 1004, 1013 (9th Cir. 2001).

In *MGM Studios v. Grokster,* the Court found that the distributors of the Gnutella-based file-sharing program Morpheus intended to induce the users of their program to infringe copyrights, based, in part, upon a statistical sampling study showing that while over 87% of the files available on Gnutella were infringing or highly likely to be infringing "[a]lmost 97% of the files actually requested for downloading were infringing or highly likely to be infringing."[17]

More recently, Illinois State University's "Digital Citizen Project" conducted disclosed monitoring of campus use of a broad range of file-sharing programs and protocols like those at issue in the *Comcast Network Management Order*.[18] The study disclosing the results of that monitoring reached clear conclusions:

- "[W]e found no evidence that large numbers of students use P2P for these legal purposes and not to transfer copyrighted material."
- "Most users are intensive users of P2P to transfer copyrighted material."
- "Some might suggest that there are many people who use P2P for the legal transfer of software, such as Linux, or for the transfer of adult material (which may or may not be copyrighted), but do not engage in the illegal transfer of copyrighted material. However, we found no evidence of this among college students."
- "[A]s for the legal transfer of software, the percentage of P2P users found transferring Linux out of those that do not transfer copyrighted media is not statistically different from zero."[19]

Finally, in *Columbia Pictures, Ind., Inc. v. Fung,* the Court found that the operator of very widely used BitTorrent tracker sites including Isohunt intended to induce copyright infringement, again, based in part upon a statistical sampling study showing that "approximately 95% of downloads occurring through Defendants' sites are downloads of copyright-infringing content."[20]

In particular, the statistical analyses in *Grokster* and *Fung* and the results of Digital Citizen's campus-wide P2P monitoring study have particular significance for the Commission. During the last Administration, three Commissioners, citing no adequate supporting data, declared that although once

---

[16] In re Aimster Copyright Litigation, 334 F.3d 643, 650 (7th Cir. 2003).
[17] MGM Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 985 (C.D. Cal. 2006).
[18] I discussed the tension between the Order and the Digital Citizen Project study in my blog post An Interesting P2P Usage Study from ISU's Digital Citizen Project http://blog.pff.org/archives/2009/03/print/005503.html.
[19] Alexandre M. Mateus & Jon M. Pena, Dimensions of P2P and Digital Piracy in a College Campus, 1, 21, 29 (TPRC 2008) http://digitalcitizen.illinoisstate.edu/press_presentations/documents/mateus-peha-TPRC-paper.pdf
[20] Order Granting Plaintiffs' Motion for Summary Judgment on Liability, Columbia Pictures, Ind., Inc. v. Fung, CV 06-5578 SVW (JCx) (C.D. Cal. Dec. 21, 2009) (slip op.).

relegated to serving *mostly* "unsavory or even unlawful purposes," "BitTorrent and other peer-to-peer technologies, such as Gnutella, have entered the mainstream."[21]

The data cited above show that this claim is no more plausible today as it was when it was made.

The Commission should find the preceding statistical data both stunning and enlightening. Nothing about a program like Morpheus or a website like Isohunt would *require* their users to use them unlawfully. Nevertheless, in both *Grokster* and *Fung,* federal courts credited and relied upon statistical evidence that both were probably used for unlawful purposes at least 95% of the time.

Nor do the statistical analyses that these Courts found credible suggest that 95% of persons using this program and website were using them for exclusively unlawful purposes while 5% were using them for exclusively lawful purposes. To the contrary, the results of these studies are so lopsided that they prove that it is far more likely than not that nearly 100% of those using this program and website were using them *almost exclusively* for unlawful purposes—though some incidental lawful uses were sometimes made. Predictably, the Digital-Citizen study—which reached similar conclusions by studying a much broader array of file-sharing programs and protocols—strongly tends to confirm this interpretation of the others. Collectively, these data should suggest three conclusions highly relevant to the future of the NPRM.

First, available data about applications, services, and devices used predominantly for unlawful purposes shows that difficult questions of degree or judgment should rarely arise were the Proposed Rules narrowed to protect only providers and subscribers using applications, services and devices used for predominantly lawful purposes. Real-world data has confirmed what common-sense would already suggest: as in the brick-and-mortar world, the needs of lawful and unlawful *Internet* commerce differ so radically that the Commission can expect few difficulties administering neutrality rules that protect only applications, services, and devices used for predominately lawful purposes—particularly if their providers or users must bear the burden of proving that lawful uses predominate.

For example, even though BitTorrent-based applications and services differ significantly from the FastTrack and Gnutella-based applications at issue in *Grokster,* Judge Wilson easily concluded in *Fung* that tracker-sites like Isohunt were no different from piracy-adapted file-sharing programs like Grokster and Morpheus or services like Napster—just "old wine in a new bottle."

Second, available data about applications, services, and devices used predominantly for unlawful purposes suggests that applications, services, and devices used for predominantly unlawful purposes today are unlikely to blossom into productive, lawful uses tomorrow. Indeed, available evidence quite clearly suggests that the needs of lawful and unlawful commerce differ so radically that it is highly unlikely that such a shift would occur in practice. Moreover, reasonable laws cannot prevent private parties from discriminating against those who do more harm than good *today* just because they *might* do more good than harm tomorrow.

[21] Comcast Network Management Order, at ¶ 4 (emphasis added).

Third, available data about how applications, services, and devices used predominantly for unlawful purposes are actually used in practice suggests that the Commission must take a harshly skeptical view of comments and testimony that stress the oh-so-many "non-infringing uses" of piracy-adapted applications and services like Morpheus and Isohunt or functionally similar applications or services. Such uses predominate only in the advocacy of certain "public interest" groups, not in reality.

Can such applications and services be used lawfully? Of course: presumably, not even the most malign would-be-pirate-king lurking on the Internet would be so unwise as to design any means of copying or distributing files that was wholly *incapable* of at incidental lawful uses. Are such applications and services sometimes used lawfully? Of course: in addition to rare incidental lawful uses, zealots can *choose* to make a point of using piracy-adapted file-sharing programs for some lawful purpose for which they will tend to be ill-suited.

For example, can you use a Gnutella-based file-sharing program like Shareaze or LimeWire to distribute public-domain recordings of barbershop quartets? Of course you can—although doing so makes about as much sense as using a screwdriver to pound nails. And that is why such uses are so rare in practice—most people don't bother to use screwdrivers to pound nails. Professor Tim Wu once explained what is really going on here:

> It is important to realize that pure "peer-to-peer" filesharing programs are not necessarily the best systems of online distribution. Their popularity and comparative advantage lies in the fact that they are designed to evade copyright's enforcement system, and therefore minimize the price of an essential input (copyrighted materials).[22]

A developer of the Gnutella-protocol based file-sharing program LimeWire put the same point more concretely: "Here's modern p2p's dirty little secret: It's actually horrible at rare stuff.[23] Nor is this the

---

[22] Timothy Wu, Copyright's Communications Policy, 103 Mich. L. Rev. 278, 361 (2004); see also Tim Wu, When Code Isn't Law, 89 Va. L. Rev. 679, 731-37 (2003) (describing efforts to "program around" copyright law); id. at 717 ("P2P design shows that avoiding copyright requires important deviations from the optimal design for speed, control, and usability"); Tim Wu, The Copyright Paradox, 2005 Sup. Ct. Rev. 229, 239 (arguing that theoretically "neutral" programs like Kazaa and Grokster "have always been understood not just as a means of disseminating information, but as a way to get music and sometimes movies for free"). These realities were, however, often denied by uninformed Internet gadflies and demagogues. See, e.g., Lawrence Lessig, Free Culture 17 (Penguin Press 2004) (claiming that file-sharing programs are "among the most efficient of the efficient technologies that the Internet enables"); Mark N. Cooper, Time for the Recording Industry to Face the Music, 4 (Consumer Federation of America, Public Knowledge, Free Press, et. al., March 2005) http://www.consumerfed.org/pdfs/BENEFITSofPEERtoPEER.pdf (predicting that the Supreme Court would dismiss all claims against the Grokster Defendants because "network efficiency is the driving force behind architectural design" and "[P2P] filesharing is among the most efficient of the efficient technologies the Internet enables").

[23] Kevin Faaborg, Losing the Long Tail, LimeWire Blog (July 13, 2006) at www.limewire.org/blog/?cat=29. He levels a similar accusation at BitTorrent: "BitTorrent is horrible at rare stuff! As soon as a files becomes rare, it looses [sic] seeders and dies." Id

only reason that you would rarely, as a practical matter, *want* to use similar file-sharing programs to lawfully acquire content that you could almost certainly acquire more quickly and safely through some other means.[24]

In conclusion, real-world experience has repeatedly confirmed what common sense should also suggest: the needs of lawful and unlawful Internet commerce differ so radically that, in practice, the Commission would rarely encounter "close cases" in which it was difficult to tell whether a given OSP's application, service or device was used predominately for lawful purposes.

b) Experience has repeatedly proven that applications, services, and devices used predominantly for unlawful purposes tend to become far more malign than theory would suggest.

The preceding data shows that applications and services suited for unlawful uses will tend to be used, in practice overwhelming for unlawful purposes—because lawful and unlawful commerce tend to have such vastly different needs. Unfortunately, different *types* of unlawful commerce often have fairly similar needs. Consequently, in practice, questionable applications have tended to impose risks both more broad and severe than an abstract tally of lawful/unlawful uses would suggest.

(1) Meet FreeNet 0.67, MUTE and TOR, some of the Russian-Roulette applications that the Proposed Rules would protect.

To understand why the NPRM's Proposed Rules are not reasoned, consider FreeNet 0.67, MUTE, and TOR. Today, each should qualify as a "lawful" application or service against which ISPs should, presumptively, not discriminate. Nevertheless, no reasonable ISP subscriber who understood the risks inherent in these applications would go have anything to do with them. These applications are "lawful," but frighteningly dangerous. Moreover, while they might seem to differ, they and other applications and services create the same fundamental hazard.

FreeNet 0.67 contains a true forced-sharing feature: Every user of FreeNet must share files; the program itself decides which files a given user will share, and it copies them onto the user's hard drive.

By contrast, MUTE is a "proxying" file-sharing program designed specifically for copyright piracy. Its developer once explained that MUTE "helps people break the law." He admitted this openly: "Sure many other P2P developers and companies blatantly lie about what their software is for, but I refuse to lie."[25] But he was less open about admitting that if you install MUTE, you may facilitate illegal activities worse than copyright infringement. Indeed, the distributor of an open-source MUTE-clone once

[24] Thomas D. Sydnor II, John Knight & Lee A. Hollaar, Filesharing Programs and "Technological Features to Induce Users to Share" 10 (U.S. Patent & Trademark Office 2007) (discussing other risks that would discourage lawful uses like "sharing" family photos).

[25] Howard Wen, Open Source P2P with MUTE, ONLAMP.COM, Aug. 12, 2004, http://www.onlamp.com/pub/a/onlamp/2004/08/12/mute.html?page=1; MUTE, How File Sharing Reveals Your Identity, at http://mute-net.sourceforge.net/howPrivacy.shtml (last visited Sept. 18, 2006).

explained that users just should not think about whether they were distributing child pornography because "with this way of reasoning, people should still live in caves."[26]

TOR is a so-called "onion router": *sometimes*, it can conceal the source or the destination of files being transferred by routing them indirectly through the computers of unknown third parties. And like FreeNet 0.67, its design and open-source code mean that for real dissidents, TOR may or may not be helpful because it *could* route their communications to the headquarters of the Secret Police. Shockingly, first-world copyright pirates and pedophiles—who will be killed if detected—do reportedly find TOR more useful.[27]

Nevertheless, only by digging deep into an associated forum for one of these three applications could a potential user get a good hint as to why all three are so dangerous. Nevertheless, only in an obscure FreeNet-related FAQ did the distributors of FreeNet hint at the real dangers:

> **I don't want my node to be used to harbor child porn, offensive content or terrorism. What can I do?**
> The true test of someone who claims to believe in Freedom of Speech is whether they tolerate speech which they disagree with, or even find disgusting. If this is not acceptable to you, you should not run a Freenet node.[28]

In other words, you can only run a program like FreeNet *if* you are willing to "harbor" pedophiles or terrorists by helping them complete their illegal acts, or, for that matter, willing to aid-and-abet any other sort of crime that someone else might want you and your computer to facilitate. If one terrorist or pedophile uses any of these applications, then any user of any of these applications can distribute sadistic child pornography or terrorists' plans to slaughter civilians. And, to be clear, in the case of piracy-adapted file sharing programs, the term "sadistic child pornography" is not exaggerated. As District Attorney Thomas Spota has warned:

> The images of child pornography available on peer-to-peer networks are some of the worst seen by law enforcement to date…. [I]n one case,… there is a child being heard saying ''No, Daddy, stop, no, Daddy,'' in a futile attempt to prevent being raped.[29]

Nor could any FreeNet user assume that they would be held blameless for personally facilitating pedophilia or terrorism just because the illegal files that they distributed were weakly encrypted: this encryption merely provided "plausible deniability"—the same see-no-evil scheme that backfired when attempted before Judge Richard Posner.[30] Unfortunately, the familiar legal implications of plausible

---

[26] See Michael Ingram, Ants P2P2P: A New Approach to File-Sharing, SLYCK NEWS, Sept. 13, 2004, http://www.slyck.com/news.php?story=567.
[27] Robert Lemos, Tor Hack Proposed to Catch Criminals, SecurityFocus March 8, 2007, http://www.broadbandreports.com/shownews/Cleaning-Up-Tor-82218.
[28] FreeNet, Frequently Asked Questions, http://freenetproject.org/faq.html#legal.
[29] Pornography on the Internet: A Hearing Before the S. Comm. on the Judiciary, 108 Cong. 10 (2003) (statement of Thomas J. Spota, Suffolk County District Attorney).
[30] In re Aimster Copyright Litigation, 334 F.3d 643, 650 (7th Cir. 2003).

deniability, (that is, of not looking because you know that you might go to prison if someone could prove that you *did know* what you were facilitating), somehow evaded the crack team at FreeNet, who were thus providing the following cheery legal advice to any teenage children of any subscribers of any American ISPs who might install or run their program:

> We have done everything we can to make it extremely difficult for any sane legal system to justify punishing someone for running a Freenet node, and there is little precedent for such action in today's developed countries. Many legal systems recognise [sic] the importance of freedom of speech....[31]

Nevertheless, FreeNet's developers did note that in countries that do not seem to prohibit or discourage ISPs from discriminating against all lawful applications and services, "your ISP or hosting provider may have a problem with Freenet."

But the Proposed Rules would reduce the risk that such a thing would happen here in America—a country in which a law-enforcement agency has *already* denounced and tried to punish an ISP from discriminating against applications and services that *could* be used lawfully, without investigating how *often* the applications at issue were actually used lawfully in practice.[32] Under the Commission's Proposed Rules, FreeNet 0.67, MUTE, and TOR are all "lawful" applications that ISPs could discriminate against only at their peril: all distributors or users of all such lawful Russian-roulette applications would be protected, deputized enforcers of "open Internet principles" empowered to deter potential wrongdoing by American ISPs.

But that is also why those Proposed Rules are unreasoned "mush." No federal law-enforcement agency should have to waste private and public resources by dragging private ISPs through one or more adjudications just to assure the agency in question that it really is probably reasonable for ISPs inclined to do so to "discriminate" against applications like these. Such questions can be resolved, *ex ante*.

Fortunately, for all concerned, FreeNet 0.67, MUTE, and TOR are NOT widely used programs: for now, they are slow and inconvenient, and thus, rarely used in practice. Consequently, this discussion of them could raise concerns about selection bias. More bluntly, some might worry that I am unfairly smearing the *class* of applications or services used predominantly for unlawful purposes by discussing rare, extreme members that conduct cannot be presumed to reflect the behavior of more popular, mainstream applications or services that happen to be used predominantly for unlawful purposes.

I agree that reasoned decisionmakers should always be alert to the risk of selection bias by commenters or litigants. Indeed, that is why these comments warn about those who pound nails with screwdrivers.

---

[31] FreeNet, Frequently Asked Questions, http://freenetproject.org/faq.html#legal.

[32] See generally, NPRM at ¶ 123 & N. 240 (explaining that while U.S. ISPs may once have been blocking or delaying the sort of BitTorrent-based file-sharing programs used in connection with tracker sites like The Pirate Bay, Mininova, and Isohunt, such ISP conduct "was largely absent at the beginning of 2009, after the Comcast Network Management Practices Order was issued"). But see NPRM ¶ 139 ("open Internet principles apply only to lawful transfers of content").

Fortunately, here, concerns about selection bias can be resolved by focusing on the evolution of LimeWire, the most widely used and "mainstream" piracy-adapted file-sharing program yet known.

In short, focusing on LimeWire will not only answer concerns about selection bias, it will even provide some perspective on FreeNet, MUTE, and TOR. In theory, the latter applications are frightening, and could obviously cause grave harm. In practice, LimeWire and similar programs have caused grave harm on scales and in ways previously unimaginable.

After all, LimeWire empowered convicted identity thieves. LimeWire exposed the schematics and passwords for the Pentagon's secret computer backbone. LimeWire achieved such results by incorporating into its program "technological features to induce users to share" that were so widely known to cause the sort of data-security disasters that they soon caused *again* in LimeWire that its distributors had already drafted and promised to abide by a self-regulatory *Code of Conduct* that they then promptly violated. And it was the combination of LimeWire and trusting little girls that subjected both the Chief Privacy Officer of the Department of Transportation to a federal investigation and the Bucci family to identity theft.

Indeed, focusing on LimeWire could be not only legally, but practically useful to the Commission and its staff. After all, every Commissioner and Commission employee can rest assured: if you or any child, spouse, partner, significant other, nanny, baby-sitter, maid, relative or friend of yours is or has ever used YOUR computer and/or YOUR Internet-access service to run a piracy-adapted file-sharing program similar to some of those at issue in the *Comcast Network Management Order*, then three conclusions follow.

First, that program was probably a version of LimeWire. Second, you can be all-but certain that your Internet-access account was NOT being used exclusively for those lawful purposes for which such programs tend to be so ill-suited. Third, should a piracy adapted file-sharing program like LimeWire cause you to start broadcasting sensitive federal data over the Internet, be assured that although the House Committee on Ethics just fired a diligent staffer who made the career-ending mistake of using a piracy-adapted file-sharing program on his home computer, some federal employees have been retained after a thorough investigation of their actions and home computers by the relevant Inspector General.

Unfortunately, in the unlikely event that the preceding paragraphs might actually cause some Commissioner or Commission staffer reading them to rush home, examine each computer connected to his or her own broadband Internet-access account, and discover something as unfortunate as LimeWire, that person should be warned: Don't make the "newbie" mistake made so often by security experts, major universities, journalists, and the Bucci family profiled by Today Investigates. Don't think that you can *really* end your LimeWire problem and protect your children, savings and career by promptly removing or deleting the program from your computer.

Distributors of many piracy-adapted file-sharing programs saw that coming. Indeed, they have known for *years* that parents and employers in the country would engage in such "discrimination" were they to

discover on one of their own computers a piracy-adapted file-sharing program that was both potentially dangerous and/or almost never used mostly for lawful purposes.

So many of them made sure that this response would not work. They *very* deliberately designed their programs to ensure that simple corrective measures like deleting or removing their programs from your computer won't end your problem.[33] To the contrary, simply deleting or removing their programs will merely turn your computer into a ticking time-bomb. Unfortunately, should that bomb go off 2010, it appears that it may now explode upon you, your finances, your children, and/or your career even more quickly than it might have back in 2008.[34]

Nevertheless, the distributors of LimeWire would be within the class of "lawful" OSPs deputized by the Proposed Rules to protect the "open Internet" from broadband ISPs who might someday do something that would impede the development of an open and law-abiding Internet.

(2) Meet LimeWire, a "lawful" and mainstream beneficiary of the Proposed Rules.

I have published, blogged, and testified extensively about why piracy-adapted file-sharing programs that are used mostly to make and distribute infringing copies of popular music and movies have caused such severe harm to so many social interests other than those of America's world-leading creators and creative industries.[35] And while my testimony and writings have often focused on a piracy-adapted file-sharing program called "LimeWire," that is not because its distributors seem to have behaved differently from the distributors of many other functionally similar file-sharing programs. To the contrary, their behavior seems about average when compared to that of distributors of functionally similar programs.

Nevertheless, there are good reasons why LimeWire can best illustrate how applications and services used predominantly for unlawful purposes will tend to behave, evolve, and affect their users and society. First, LimeWire is now the most widely used file-sharing program, so its behavior will affect many users, their families, and the employers of members of their families. Second, LimeWire has been a long-lived program, so it can show us how such a program evolves over nearly a decade. Third, several other fairly popular file-sharing programs are "forks" of LimeWire's open-source code, so analyses of how LimeWire behaves can reveal how some other relatively popular file-sharing programs may behave.

---

[33] See Thomas D. Sydnor II, John Knight & Lee A. Hollaar, Filesharing Programs and "Technological Features to Induce Users to Share" 31-32 (U.S. Patent & Trademark Office 2007) (discussing "partial-uninstall" features); Thomas D. Sydnor II, John Knight & Lee A. Hollaar, Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform, 10-11 (PFF 2007) (same); Thomas D. Sydnor II, Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5, 18-20 (PFF 2009) (same).

[34] See NPRM ¶ 123 & n.240.

[35] See Thomas D. Sydnor II, John Knight & Lee A. Hollaar, Filesharing Programs and "Technological Features to Induce Users to Share" (U.S. Patent & Trademark Office 2007); Thomas D. Sydnor II, John Knight & Lee A. Hollaar, Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform (PFF 2007); Thomas D. Sydnor II, Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5 (PFF 2009).

For these reasons, LimeWire provides a good case study that illustrates a broader point: When applications and services are used predominantly for unlawful purposes, like copyright infringement, they have proven to be far more harmful in fact than any abstract balancing of percentages of unlawful and lawful uses might suggest. In particular, three sorts of further harm seem particularly widespread and malign.

First, applications and services used predominantly for unlawful purposes deter *productive* innovation and the growth of the lawful commerce that generates jobs and sustained economic growth. On the Internet today, not only is rampant copyright piracy endangering an increasingly wide array of our often world-leading creative industries, it is also endangering or harming the innovative American OSPs who are trying to build *law-abiding* Internet content-distribution applications and services. Indeed, I strongly commend the Commission for

Second, applications and services used predominantly for unlawful purposes have too often inflicted upon both their users and many others, conduct that arguably might involve deliberate *fraud*. It is not difficult to imagine why.

Well-designed federal laws should create powerful disincentives to behave unlawfully. Granted, these disincentives might be overcome if a person thought that they could get away with an illegal act that would benefit *them.* For example, someone might *choose* to steal if they concluded that the financial benefits of the theft exceeded the cost of the likely legal penalty divided by the odds of getting caught. But a similar cost-benefit analysis should make it *very* difficult to convince someone to break the law in a way that does not directly benefit them.

Consequently, it should be relatively easy to tempt users of file-sharing programs to download infringing files that they do not already possess—but very difficult to convince them to *voluntarily* "share" lots of files that they already possess or to cripple their own computer by housing a database of files being shared by thousands of anonymous strangers. Only in the latter two contexts have many distributors of piracy-adapted file-sharing programs repeatedly behaved in ways that could arguably reflect intent to dupe vulnerable users—like teens and preteens—into sharing files inadvertently or housing databases of files being shared by anonymous strangers.

Third, applications and services used predominantly for *one* unlawful purpose often facilitate other unlawful acts that they were almost certainly never *intended* to facilitate. The needs of lawful and unlawful exchange tend to differ radically, but the needs of various forms of unlawful exchange tend to be similar.

For example, in *Grokster,* the courts found "overwhelming" and "clear" evidence that the distributors of the Gnutella-protocol- based file-sharing program Morpheus intended to induce, (i.e., encourage or dupe), users of their program into infringing copyrights. These findings from *Grokster* could thus suggest that distributors of functionally similar Gnutella-protocol-based file-sharing programs like LimeWire, FrostWire or Shareaza might harbor similar intent to induce copyright infringement. But neither *Grokster* nor other evidence known to me suggests that any distributor of any Gnutella-based file-sharing program ever *intended* to induce identity theft, the rape of a toddler, or innumerable

breaches of personal, corporate, national, and military security—including the disclosure of risk assessments that would show terrorists how to attack Chicago and other cities in the way that would kill the most American civilians.

Nevertheless, these are all documented consequences of LimeWire or fundamentally similar piracy-adapted file-sharing programs. Often, these consequences were just the long-known effects of "features" that tended to trick users into sharing all or most of their personal data files, which would tend to include not only financial and work-related documents, but also entire collections of popular music. Moreover, all of these unlawful uses could have been nearly eliminated or swiftly remedied by simple measures routinely implemented in Internet applications and services designed for *lawful* commerce. Such measure could include (1) ensuring that misbehaving users can be barred from the system, and (2) ensuring that unauthorized or dangerous files can be quickly removed from the system.

Unfortunately, these obvious solutions that could have thwarted identity thieves, pedophiles, malware distributors, and a potential crazed assassin of the President's children were never adopted by the distributors of LimeWire. Only they know why they never implemented simple measures that could have significantly deterred identity theft, data breaches, and the distribution of child pornography—but also *infringing* uses of LimeWire.

Nevertheless, even in a worst-case scenario in which a court were someday to cite *Grokster* and *Fung* and hold that LimeWire was just more "old wine in a new bottle" distributed by people who *intended* to induce users of their program to infringe copyrights, not even that holding would suggest that the many non-infringement-related effects of LimeWire were really *intended.* Even then, there would be little reason to suspect that identity theft; breaches of national, military, corporate and personal security; distribution of child pornography; reduced sentences for sadistic pedophiles; and potential political assassinations, child abductions, and optimally murderous terrorist attacks were really *intended* consequences of LimeWire or a similar program. Even in this hypothetical, they would probably have been just the costs of "free music"—the collateral damage that distributors had every reason to know would inevitably be caused by "features" that may only have been *intended* to trick children, teenagers, students and others into illegally "sharing" more pop music.

As a result of these factors and others, LimeWire and other applications and services used mostly for unlawful purposes have caused and should be expected to continue to cause widespread harm. During the past nine years, an array of published studies, congressional hearings, and media reports have documented the breadth, severity, and probable causes of these harms. Appendix A to these comments provides an organized collection of the most significant hearings, studies, and selected media reports. Rather than recount them all in detail, these comments will summarize the most important data relating to two of these many documented harms.

Inadvertent sharing of your music collection—and all of your other sensitive personal data:

Since at least 2001, distributors of popular file-sharing programs have been incorporating into their programs certain "features" that they knew or should have known would tend to trick users into sharing all of the personal data files stored on their computer.

The breadth of the harm thus done to the government, to corporations, and to families is described in detail throughout Appendix A. Among many other things, inadvertent sharing compromised the safety of the families of Presidents Obama and Bush. It disclosed risk assessments that endangered entire cities, the Pentagon's secret computer backbone, the plans for a new Marine One helicopter for President Obama, and terabytes of data on the Joint Strike Fighter.[36]

Empowering pedophiles and endangering children

Sadly the same features that make programs like LimeWire attractive to children who want "free music" also make such programs attractive to pedophiles who want to share child pornography. For example, a joint federal-state task force recently prepared a report finding that in the state of Virginia alone, almost 20,000 computers were "sharing" illegal child pornography.[37] Some of that child pornography is also mislabeled to look like a file that would be attractive to children.

Worse yet, some of those sharing child pornography are truly dangerous.[38] And worse still, they have discovered that the problem of inadvertent sharing that has wrecked such havoc on governments, businesses, and families is a two-fold boon for pedophiles.

First, it can provide an early release by ensuring that even the worst predator cannot be convicted of *knowingly* distributing child pornography. For example, in *United States v. Park,* a LimeWire user was "sharing," *inter alia,* a three-hour video of the rape of a little girl "bound with a rope and being choked with a belt by what appeared to be an adult male.'" Nevertheless, he secured a reduced sentence because he "lacked an understanding of the software and thus … the knowledge to distribute the illegal wares that he possessed."[39]

Second, the data-security company Tiversa has warned that pedophiles have discovered that inadvertently shared collections of family photos can help them select and locate potential new victims.

---

[36] Inadvertent File-Sharing Over Peer-to-Peer Networks: *Hearing Before the H. Comm. on Oversight and Government Reform,* 110 Cong. (2007); Inadvertent File Sharing over Peer-to-Peer Networks: How It Endangers Civilians and Jeopardizes National Security: *Hearing Before the H. Comm. on Oversight and Government Reform,* 111 Cong. (July 29, 2009) http://oversight.house.gov/index.php?option=com_content&task=view&id=2465&Itemid=2

[37] Chris L. Jenkins, Officials Find Child Pornography on 20,000 Va. Computers, The Washington Post, VA03 (Apr. 10, 2008) (reporting on the results of a state-level report prepared by federal agents) at http://www.washingtonpost.com/wp-dyn/content/article/2008/04/08/AR2008040803930.html.

[38] See, e.g., United States v. Park, 2008 U.S. Dist. LEXIS 19688, (D. Neb. March 13, 2008) (a LimeWire user shared videos of an adult raping a little girl "bound with a rope and being choked with a belt"); United States v. O'Rourke, 2006 U.S. Dist. LEXIS 1044 (D. Ariz. Jan. 12, 2006) (a LimeWire user was held to be a "danger to the community" because he allegedly shared many "extraordinarily abusive" images of "horrific child abuse" inflicted on "a very young girl, with hands bound and mouth gagged"); United States v. Postel, 524 F. Supp.2d 1120, 1123 (N.D. Iowa 2006) (a LimeWire user used shared child pornography to "groom" the girl that he molested for four years).

[39] 2008 U.S. Dist. LEXIS 19688 (D. Neb. March 13, 2008).

> [C]hild… predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers…. [T]hese individuals will [then]… download all additional information being shared from that computer…. This accompanying information can be used by the predator to locate… the potential victim.[40]

In conclusion, reservations about jurisdiction and notice notwithstanding, I applaud the goal of the open and law-abiding Internet set forth in the NPRM. But I respectfully submit that this goal could be better pursued were the Proposed Rules narrowed to protect only users and providers of applications, services used for predominantly lawful purposes. Simply put, it seems impossible to conclude that entities that engage in the type of conduct described above are either worthy of unprecedented legal protections or likely to help guide us, in practice, toward an open and law-abiding Internet.

[40] See infra, n.**Error! Bookmark not defined.**.

APPENDIX A

SOURCES ON INADVERTENT FILE-SHARING

HEARINGS AND TESTIMONY:

Overexposed: The Threats to Privacy and Security on Filesharing Networks: *Hearing Before the H. Comm. on Government Reform,* 108 Cong. (2003).

The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-Peer File-Sharing Networks?: Hearing Before the S. Comm. on the Judiciary, 108 Cong. (2003).

Inadvertent File-Sharing Over Peer-to-Peer Networks: *Hearing Before the H. Comm. on Oversight and Government Reform,* 110 Cong. (2007).

H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act: Hearing Before the Subcomm. On Commerce, Trade, and Consumer Protection (May 5, 2009) http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1608:energy-and-commerce-subcommittee-legislative-hearing-on-hr-2221-the-data-accountability-and-trust-act-and-hr-1319-the-informed-p2p-user-act&catid=129:subcommittee-on-commerce-trade-and-consumer-protection&Itemid=70; Prepared Statement of Thomas D. Sydnor II (May 5, 2009) http://www.pff.org/issues-pubs/testimony/2009/090505_P2P_sydnor_testimony.pdf;

Inadvertent File Sharing over Peer-to-Peer Networks: How It Endangers Civilians and Jeopardizes National Security: *Hearing Before the H. Comm. on Oversight and Government Reform,* 111 Cong. (July 29, 2009) http://oversight.house.gov/index.php?option=com_content&task=view&id=2465&Itemid=2; *see also Written Testimony of Thomas D. Sydnor II* (July 29, 2009) http://www.pff.org/issues-pubs/testimony/2009/090729-sydnor-testimony-p2p-inadvertent-filesharing.pdf.

STUDIES:

Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing* (2002) (causes) *reprinted in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, vol. 5, iss. 1 at pp. 137-144 http://www.hpl.hp.com/techreports/2002/HPL-2002-163.pdf

Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Filesharing Programs and "Technological Features to Induce Users to Share"* (U.S. Patent & Trademark Office 2007) http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf

M. Eric Johnson, *Inadvertent Disclosure—Information Leaks in the Extended Enterprise* (WEIS 2007) http://weis2007.econinfosec.org/papers/43.pdf

Thomas D. Sydnor II, John Knight & Lee A. Hollaar, *Inadvertent Filesharing Revisited: Assessing LimeWire's Responses to the Committee on Oversight and Government Reform* (PFF 2007) http://www.pff.org/issues-pubs/pops/pop14.22inadvertentfilesharing.pdf

M. Eric Johnson, *The Evolution of the Peer-to-Peer File-Sharing Industry and the Risks to Users,* (Int'l Conf. on Sys. Sciences, 2008) http://csdl2.computer.org/comp/proceedings/hicss/2008/3075/00/30750383.pdf

Alexandre M. Mateus & Jon M. Pena, *Dimensions of P2P and Digital Piracy in a College Campus* (TPRC 2008) http://digitalcitizen.illinoisstate.edu/press_presentations/documents/mateus-peha-TPRC-paper.pdf

M. Eric Johnson, *Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain,* 25 J. OF MAN. INF. SYS. 97-123 (Fall 2008) http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JMIS08.pdf

M. Eric Johnson, *Data Hemorrhages in the Heath-Care Sector,* LECTURE NOTES IN COMPUTER SCIENCE (April 2009) http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/JohnsonHemorrhagesFC09Proceedingd.pdf

Thomas D. Sydnor II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF 2009) http://www.pff.org/issues-pubs/pops/2009/pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf

SELECTED MEDIA REPORTS ON INADVERTENT FILE-SHARING

Department of Homeland Security, *Unauthorized Peer to Peer (P2P) Programs on Government Computers* (April 19, 2005) https://secure.infragard-ct.org/public/newsfiles/Unauthorized_Peer_to_Peer_(P2P)_Programs_on_Government_Computers__April_19_2005_V6_0.pdf (warning, "Multiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P.").

Today Investigates, *New warnings on cyber-thieves,* at http://today.msnbc.msn.com/id/26184891/vp/29405819%2329405819 (reporting on inadvertent sharing of over 150,000 tax returns in New York State alone, including the Bucci family's return, which was downloaded by an identity thief who used it to steal their refund).

Jaikumar Vijayan, *Leaked House Ethics document spreads on the Net via P2P*, ComputerWorld Security (Oct. 30, 2009), http://www.computerworld.com/s/article/9140154/Leaked_House_Ethics_document_spreads_on_the_Net_via_P2P.

Jaikumar Vijayan, *House bill seeking government P2P ban gets boost*, ComputerWorld Government (Oct. 5, 2009), http://www.computerworld.com/s/article/9138958/House_bill_seeking_government_P2P_ban_gets_boost (Tiversa found some 200 incidents of sensitive military documents being available on public peer-to-peer networks).

Jaikumar Vijayan, *Details on presidential motorcades, safe house for First Family, leak via P2P*, ComputerWorld Security (July 29, 2009), http://www.computerworld.com/s/article/9136053/Details_on_presidential_motorcades_safe_house_for_First_Family_leak_via_P2P.

Jaikumar Vijayan, *Update: Strike Fighter data was leaked on P2P network in 2005, security expert says*, ComputerWorld Security (May 5, 2009), http://www.computerworld.com/s/article/9132571/Update_Strike_Fighter_data_was_leaked_on_P2P_network_in_2005_security_expert_says_.

Jaikumar Vijayan, *Classified data on president's helicopter leaked via P2P, found on Iranian computer*, ComputerWorld Security (Mar. 2, 2009), http://www.computerworld.com/s/article/9128820/Classified_data_on_president_s_helicopter_leaked_via_P2P_found_on_Iranian_computer.
Jaikumar Vijayan, *Download music, share bank account info for free on P2P networks*, ComputerWorld Security (Jun. 12, 2007), http://www.computerworld.com/s/article/9024406/Download_music_share_bank_account_info_for_free_on_P2P_networks.

David Kravets, *Men Charged With Hijacking DOD Paychecks* (Dec. 9, 2009), http://www.wired.com/threatlevel/2009/12/military-paychecks-hijacked/ (Jeffrey Girandola and Kajohn Phommavong were indicted for using peer-to-peer networks LimeWire and BearShare to obtain inadvertently shared account information for a DOD online payroll system).

Angela Moscaritolo, *Army Special Forces document leaked on P2P network*, SC Magazine (Oct. 5, 2009), http://www.scmagazineus.com/army-special-forces-document-leaked-on-p2p-network/article/151309/ (A U.S. Army Special Forces document containing the names, Social Security numbers, home phone numbers and home addresses of 463 soldiers as well as the names and ages of soldiers' spouses and children was found on a peer-to-peer network).

Declan McCullagh, *Congress: File Sharing Leaks Sensitive Government Data*, CBS News (July 29, 2009), http://www.cbsnews.com/blogs/2009/07/29/politics/politicalhotsheet/entry5195953.shtml ("Sensitive files including Secret Service safehouse locations, military rosters, and IRS tax returns can still be found on file-sharing networks, according to a report issued to a U.S. House of Representatives committee on Wednesday.")

Bob Brewin, *File-sharing networks used to uncover thousands of medical records,* nextgov (Feb. 27, 2009), http://www.nextgov.com/nextgov/ng_20090227_9147.php (A university professor was able to access medical records containing detailed personal data on physical and mental diagnoses, including one database containing records on 20,000 patients including Social Security numbers, insurance carriers, and diagnostic codes. The codes identified by name four patients infected with AIDS, the mental illnesses of 201 patients, and the cancer findings of 326 patients.)

Angela Moscaritolo, Medical data leakage rampant on P2P networks, SC Magazine (Feb. 11, 2009), http://www.scmagazineus.com/medical-data-leakage-rampant-on-p2p-networks/article/127216/.

Brian Krebs, *Justice Breyer Is Among Victims in Data Breach Caused by File Sharing*, The Washington Post (July 9, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070802997.html (An employee of a McLean investment firm installed LimeWire on a company computer and inadvertently shared the names, dates of birth, and Social Security numbers of about 2,000 of the firm's clients, including Supreme Court Justice Breyer.).

Tim Wilson, *Army Hospital Breach May Be Result of P2P Leak,* DarkReading (Jun. 3, 2008), http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201106 (The names, Social Security numbers, birth dates, and other information on more than 1,000 patients at Walter Reed Hospital was inadvertently released, likely through a peer-to-peer network).

Avi Baumstein, *Our P2P Investigation Turns Up Business Data Galore*, InformationWeek (Mar. 17, 2008), http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=206903417 (Using LimeWire, a reporter easily finds confidential business documents, Social Security numbers, credit card numbers, bank passwords, Equifax credit reports, and a handful of tax returns).

Seattle indictment highlights risks of online file sharing, KOMOnews.com (Sep. 6, 2007), http://www.komonews.com/news/9622602.html (Gregory Thomas Kopiloff used LimeWire, SoulSeek, and other peer-to-peer programs to troll other computers for financial information, which he used to open credit cards and buy more than $73,000 worth of goods online).

SELECTED MEDIA REPORTS FROM THE PAST THIRTY DAYS ON CHILD PORNOGRAPHY ON FILE-SHARING NETWORKS

FdL man guilty of child pornography possession, The Reporter (Dec. 31, 2009), http://www.fdlreporter.com/article/20091231/FON0101/912310436/1985/FONBusiness/FdL-man-guilty-of-child-pornography-possession (Timothy S. Letz pleaded no contest to two counts of possession of child pornography for sharing child pornography files via a peer-to-peer network).

YMCA Worker Part Of International Porn Case, WSMV-TV (Jan. 1, 2010), http://www.wsmv.com/news/22105885/detail.html (Daniel Quail arrested after Canadian authorities arrested someone using the same peer-to-peer network as Quail and notified American authorities).

Part-time clown and Santa sentenced to 8 years on child pornography charges, Ethiopian Review (Dec. 24, 2009), http://www.ethiopianreview.com/news/7182 (August R. Billek caught after an Immigration and Customs Enforcement agent discovered what was later identified as Billek's computer distributing child pornography via a peer-to-peer network).

Paul Luce, *Child-pornography probe snares Marcus Hook man,* Daily Times (Dec. 11, 2009), http://www.delcotimes.com/articles/2009/12/11/news/doc4b21cb74b4567667059468.txt (David Michael Walton arrested after detectives browsed his shared files on a file-sharing network).

Logan man pleads guilty to child porn, The Herald-Dispatch (Dec. 11, 2009), http://www.herald-dispatch.com/news/x456828572/Logan-man-pleads-guilty-to-child-porn (Brian P. Cornell downloaded

child pornograpy using the Internet and shared many of them through a peer-to-peer file sharing program).

Edward Van Embden, *Millville man pleads guilty to distributing child pornography*, Press of Atlantic City (Dec. 18, 2009), http://www.pressofatlanticcity.com/news/press/cumberland/article_cb8ef494-ec40-11de-8c4b-001cc4c03286.html ("Gary Gandy admitted to using a peer-to-peer file sharing service to download and distribute sexual images and videos involving children").

Amanda Terrebonne, *Paul Dixon, Michael Mammone arrested in Russellville on child porn charges*, Today's THV (Dec. 11, 2009), http://www.todaysthv.com/news/local/story.aspx?storyid=95795&catid=2 ("Police say Dixon said he had been downloading child pornography for over a year through Peer-to-Peer (P2P) networks and had accumulated about 30-50 videos showing boys as young as 10 engaged in sexually explicit conduct.").

Denise Yost, *Minister Sentenced For Distributing Child Porn*, NBC4i (Dec. 10, 2009), http://www2.nbc4i.com/cmh/news/crime/article/minister_sentenced_for_distributing_child_porn/28163/ (A FBI agent searching for people who wanted to share child pornography was contacted by Gary L. Kendall via a peer-to-peer file sharing site).

Man gets 15 years in child porn case, The Fayetteville Observer (Dec. 10, 2009), http://www.fayobserver.com/Articles/2009/12/10/959373 (Laurence David Clifton had videos depicting pre-pubescent children in sado-masochistic conduct and hundreds of other images of child pornography).

Eve Byron, *Helena man sentenced for collecting pornography images,* Independent Record (Dec. 12, 2009), http://www.helenair.com/news/local/article_54e8f066-e6e5-11de-bc00-001cc4c03286.html (Jeremy Peterson admitted that he used LimeWire to download hundreds of videos and around 12,000 images of children who were clearly prepubescent, with some engaged in sadistic or masochistic abuse or other depictions of violence).

Jim Kouri, *Kiddie porn producer exploited his own relatives*, newjerseynewsroom.com (Dec. 16, 2009), http://www.newjerseynewsroom.com/nation/kiddie-porn-producer-exploited-his-own-relatives (Michael Joseph Gilbert possessed more than 6,000 images of child pornography, including images obtained from the Internet via peer-to-peer file sharing programs and of two young relatives that he admitted making sexually explicit videos of when they were as young as 5 and 6 years old).

Jason Trahan, *UT-Arlington graduate student arrested on child pornography charges*, The Dallas Morning News (Dec. 22, 2009), http://www.dallasnews.com/sharedcontent/dws/news/city/arlington/stories/122209dnmetgradporn.377cba6.html (Sheldon Fernandes was arrested after Immigration and Customs Enforcement agents got a tip that he was downloading child pornography from peer-to-peer networks and found more than 100 videos of children in sexual situations on his computer).

Nate Robson, *Couple accused of selling drugs*, The Citizen (Dec. 22, 2009), http://www.auburnpub.com/articles/2009/12/23/local_news/news06.txt (Brien Fredendall said he unknowingly download child pornography when he used LimeWire to download adult pornography).

South Charleston Man Sentenced on Drug Charges, The State Journal (Dec. 22, 2009), http://www.statejournal.com/story.cfm?func=viewstory&storyid=72360 (James Curtis Sorgman spent more than ten years downloading over 17,000 images and videos depicting the graphic sexual abuse of children, including infants using a peer-to-peer file sharing program).